BLOG

Automated Response Across the Entire Platform: Best-of-Breed vs. Best-of-Platform

Through decades of experience in providing security solutions to customers, Bulletproof security experts have come to recognize a critical truth: the best-of-breed point solution model to secure enterprise organizations is no longer the best approach to protection.

Arming your enterprise with the "best" security point products does not ensure complete coverage in terms of security posture. In many cases, it results in coverage gaps between products. This approach can also create unnecessary overlap, leading to confusion and inconsistency in applying policies and responding to threats.

What we have learned–and lived–is that the true "best" security posture is one that tightly integrates to provide a complete, holistic picture of the organization, with no overlap or conflict in the process for investigation of or response to incidents. While other solutions can provide a "single pane of glass" for investigation, what sets this new best-of-platform model apart is the speed of incidence-to-response that automation provides.

The greatest financial impact to an organization happens in the period of time between incident detection and containment. The larger this window is, the more detrimental and costly the attack to your business. The best-of-platform approach can reduce this period of time to minutes with automated response. It provides cross-correlation between components, and automatic remediation and mitigation of security incidents.

This creates a much more effective approach to security—which, in a nutshell, demonstrates that the whole of the solution is greater than the sum of its parts. The value of the fully integrated solution with automated response is that it greatly reduces the risk that organizations face from missing a signal. It also reduces time lost to hunting through disjointed management consoles caused by siloed "best-of" products. This great reduction in risk and increase in response speed is the ROI.

Intelligent technology is well-suited to take on more repetitive tasks such as noise monitoring and low-level event handling. No one wants to miss threats by ignoring things, but human time wasted on chasing dead ends leads to longer response time for actual incidents. Automation helps correlate, consolidate, and analyze a high volume of alerts, enabling your human analysts to spend their time on investigation and remediation of complex issues. Automated response across the entire platform–which is the only chance for successful mitigation of a complex human-led breach or attack–can only be achieved by a platform that provides complete end-to-end coverage, from endpoint to infrastructure, identity to cloud.

"The threat landscape has evolved to a point where the best-of-breed model is now creating a false sense of security."

This cannot be accomplished natively within a multi-vendor EDR/SIEM offering. Every additional static integration point in a multi-vendor offering adds complexity, risk, overhead, confusion, and delay in response time.

Investigation capabilities are also vastly improved in the best-of-platform model. We can investigate through a single management console rather than through various vendor consoles for different products. With this capability, we can investigate a single collection of evidence rather than individual components. This significantly decreases the time required to investigate and respond, leaving much less time for the "bad guys" to do damage.

The threat landscape has evolved to a point where, unfortunately, the best-of-breed model is now creating a false sense of security. It creates gaps. It creates confusion. It creates additional overhead. In today's threat landscape, with a continuous increase in the volume and complexity of attacks, the ability to streamline investigation and response across your entire platform is the only viable option if you want to properly protect your business.

Our Approach to Best-of-Platform

At Bulletproof, we fulfill the promise of best-of-platform protection with the Microsoft Security platform. In our experience, it offers unmatched integration and automation.

The security industry is inundated with acronyms, and the latest to hit the market is XDR, or Extended Detection and Response. It is defined by Gartner as "a SaaS-based, vendor-specific security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components." This industry shift toward a platform approach is in recognition of the gaps that exist in the legacy best-of-breed model, particularly as it relates to response capabilities.

Microsoft has been a leader in this space well before the acronym was coined, and recently rebranded their security suite of products under the Microsoft Defender brand to better reflect the pre-existing integration across its platform.

Microsoft Defender includes coverage across all areas of a customer's computing environment, including:

- Identity (on cloud and on prem)
- Infrastructure (on cloud and on prem)
- Productivity (O365)
- Application (SQL Server)
- Endpoint (traditional and mobile)
- OT operating environments

No other security vendor can offer such a wide breadth of integrated coverage for the entire enterprise.

Integrating the Microsoft Defender toolset with Microsoft's Azure Sentinel SIEM/SOAR unlocks full end-to-end visibility across all resources (including edge network) with correlated, prioritized alerts based on the deep understanding Microsoft has of the products that it has built, its vast threat intelligence capabilities, and artificial intelligence/machine learning (AI/ML). Beyond more accurate alerting, this native integration also enables intelligent automated response and containment activities across the entire platform, something no other vendor can match.

The Microsoft Defender suite of products provides this complete solution, and when integrated together through a single pane of glass (Microsoft's Sentinel SIEM/SOAR), allows deep investigation, cross-correlation between components, and automatic remediation and mitigation of security incidents. Most SIEMs take logs from multiple sources. Azure Sentinel goes a step further. Now you can get a unified view of all those inputs in Sentinel, and seamlessly drill down into an incident in Microsoft 365 Defender.

The time differential between detection and remediation in the best-of-breed vs best-of-platform scenarios can make or break your organization. Response times under the best-of-breed model can be hours at best but can stretch into multiple days or even weeks. The cost of breach continues to rise, and studies show that automated response capabilities can cut this cost in half.

Microsoft Partner

Microsoft

2021 Partner of the Year Winner
Security Award

"Studies show that automated response capabilities can detect threats in minutes, not months."

The Biggest Benefit of Best-of-Platform: Automated Response

Human-operated ransomware campaigns pose a significant and growing threat to businesses and represent one of the most impactful trends in cyberattacks today. In these hands-on-keyboard attacks—which are different from auto-spreading ransomware like WannaCry or NotPetya—adversaries employ credential theft and lateral movement methods traditionally associated with targeted attacks like those from nation-state actors. They exhibit extensive knowledge of systems administration and common network security misconfigurations, perform thorough reconnaissance, and adapt to what they discover in a compromised network.

These attacks are known to take advantage of network configuration weaknesses and vulnerable services to deploy ransomware payloads. And, while ransomware is the very visible action taken in these attacks, human operators also deliver other malicious payloads, steal credentials, and access and exfiltrate data from compromised networks.

News about ransomware attacks often focus on the downtimes they cause, the ransom payments, and the details of the ransomware payload, leaving out details of the oftentimes long-running campaigns and preventable domain compromises that allow these human-operated attacks to succeed.

Based on our investigations, these campaigns appear unconcerned with stealth and have shown that they could operate unfettered in networks. Human operators compromise accounts with higher privileges, escalate privilege, or use credential dumping techniques to establish a foothold on machines and continue unabated in infiltrating target environments.

Human-operated ransomware campaigns often start with "commodity malware" like banking Trojans or "unsophisticated" attack vectors that typically trigger multiple detection alerts; however, these tend to be triaged as unimportant and therefore not thoroughly investigated and remediated. In addition, the initial payloads are frequently stopped by antivirus solutions, but attackers just deploy a different payload or use administrative access to disable the antivirus without attracting the attention of incident responders or security operations centers (SOCs).

The bottom line from what we've seen in the wild? Automated response is the best defense against complex human-operated attacks.

Microsoft Defender for Endpoint is the only solution that provides AI-based automated response natively, right out of the box, which can automatically investigate, evaluate, and respond to threats. The ability to respond to threats from the Defender for Endpoint portal, whether manual or automatic, is a key differentiator from other solutions. The deep integration provides visibility and control beyond what other solutions can offer.

An example of automated remediations that we have seen is a scenario in which a workstation is used to browse a website and it downloads a file which turns out to be malicious when it is executed. Defender for Endpoint can detect this and alert the Defender for EndPoint portal, where Azure Sentinel, based on policies in place, can automatically instruct the workstation to isolate itself from the rest of the network until it can be investigated thoroughly. This is just one example of how automated remediations can be used to shorten the time between detection and response of an issue.

The alternative to this is the legacy scenario, whereby a security officer or other IT personnel are alerted of a potential incident, time is spent investigating the received alert, a decision is finally made to investigate the workstation more thoroughly, and someone either manually removes the workstation from the network or makes changes to a network switch or other architecture to isolate the workstation. This takes time—time that could allow something malicious on a workstation to traverse laterally throughout the network and affect multiple devices. This is, unfortunately, the scenario that we are often faced with when using best-of-breed solutions that do not have built-in, automated response mechanisms.

The bigger issue, however, is if credentials were captured before the workstation was isolated. If there is no integration between security solutions, even though the machine has been isolated, the identities on the machine have not. This means the attacker can simply jump directly into the cloud, furthering the attack.

Defender for Endpoint is also a built-in component of Windows 10, with complete integration and visibility into the Windows OS. No other EDR/XDR can provide the same level of visibility and control on the workstation. With this built-in approach there are no agents to deploy and manage. The features already exist in the OS, which also makes them harder for bad actors to bypass or disable.

Further, Cloud Access Security Broker (CASB)-like functionality is built into Defender for Endpoint, which allows automatic protections such as blocking a workstation from accessing a malicious website that has been identified by Microsoft's Threat Intelligence. It also integrates tightly with Microsoft's CASB, Microsoft Cloud App Security, which provides additional control and visibility into a workstation/user's use of other cloud services—even non-Microsoft services like Dropbox, Salesforce, etc.

This integration of Defender for Endpoint with Microsoft Cloud App Security also allows organizations to sanction or disallow the use of certain cloud SaaS apps or services for groups of users or for all users. This can't be done with security products that aren't integrated.

Other out-of-the-box automated remediation/mitigation techniques that can be deployed on a workstation using Defender for Endpoint, which includes:

- Collect investigation package
- Isolate device (this action can be undone)
- Offboard machine
- Release code execution
- Release from quarantine
- Request sample
- Restrict code execution (this action can be undone)
- Run antivirus scan
- Stop and quarantine

Microsoft's Best-of-Platform Approach Comes With Threat Expert Access

With Defender for Endpoint, we can submit evidence to Microsoft Threat Experts for malware analysis from their highly trained resources, extending our security team beyond Bulletproof directly into Microsoft itself.

Bulletproof utilizes Threat Hunting techniques as a key component of both its reactive and proactive services within our Bulletproof 365 Enterprise service offering. Using Jupyter Notebooks, we create repeatable playbooks that can be used to perform Threat Hunting exercises. Many examples of these notebooks are being published online through the security community to help build out threat hunting toolboxes, again shortening the time to detection through sharing of vital information and techniques.

Evidence found through threat hunting, or through detections from the various sensors in the E5 Security toolset, can be correlated between Azure Sentinel, Defender for Endpoint, Defender for Office 365, and Microsoft Cloud App Security, among other components, to show the entire incident body of evidence in one pane of glass. This cannot be accomplished as easily using other non-integrated products, where we may not be as freely available to use APIs to integrate and parse data.

Defender for Endpoint also has direct integration with Microsoft Data Loss Prevention (DLP) technologies, enabling further insights and capabilities when customers are implementing Governance and Compliance controls within their organization.

Defender for Office 365 P2: Automation Beyond Email

It is no surprise that email is still the primary attack mechanism for malicious software and bad actors. Protections for email environments are paramount and considered table-stakes for most organizations' security programs. There are many competing solutions in the market that can help reduce the number of phishing emails, malicious attachments, files, and links that your users come into contact with, and many of them do a respectable job of detecting and preventing these threats from reaching your user base.

Defender for Office 365 P2 is an extremely capable mechanism that Microsoft provides to help in this regard, and it is an integral component of the Microsoft 365 Security suite. But Defender for Office 365 P2 takes its coverage further than its competitors. Not only does it protect email, but it provides protection for other productivity applications, such as OneDrive, SharePoint, and Teams. Defender for Office 365 P2 will detect when malicious files (or even web links) are pasted to these applications, removing them before users can innocently click on them and find themselves in trouble. This closes a gap that other products suffer from.

Competitor solutions focus exclusively on email, and some of them only detect malicious items as they pass through the protection gate–they can't reach into your users' mailboxes and remove links that become weaponized AFTER the email was delivered.

Defender for Office 365 P2 is very tightly integrated with the rest of the Microsoft security stack and provides automated response mechanisms to reduce the time between incident detection and response.

Defender for Office 365 provides responses to automated investigations that can include the following actions, right out of the box:

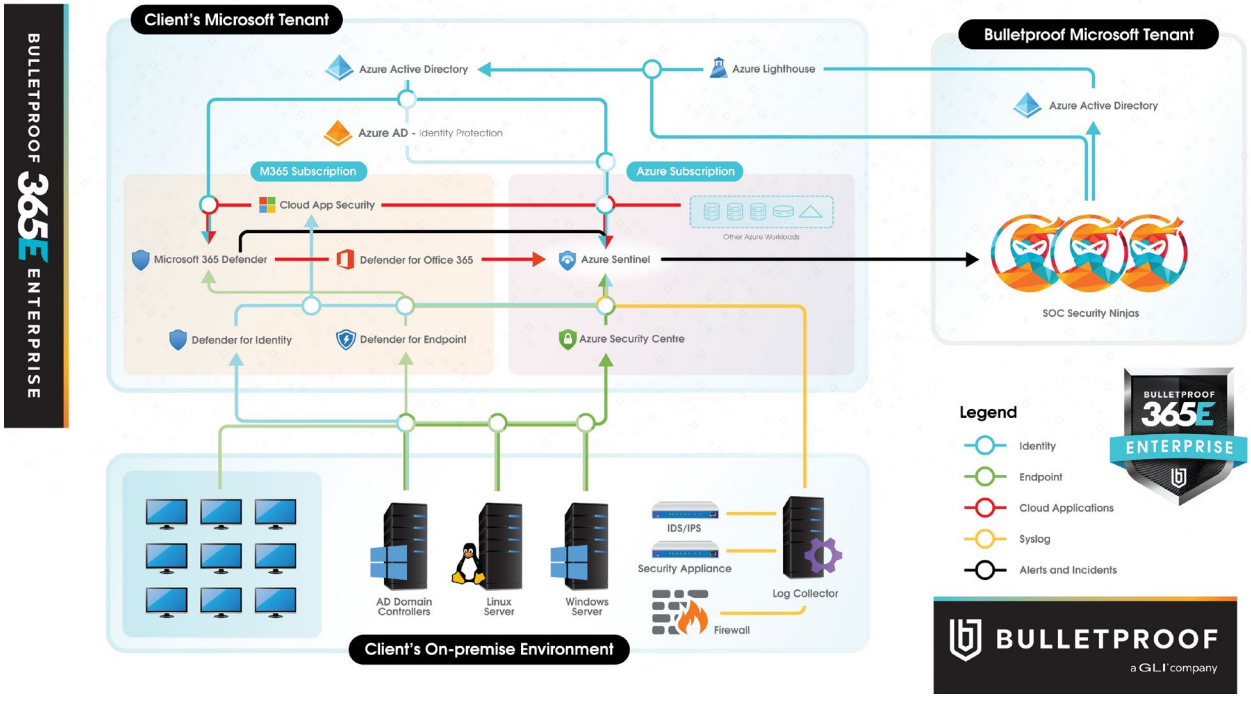
- Blocking of URLs (time-of-click): Microsoft will check out a URL before a user can access it to ensure the user does not accidentally get themselves into trouble
- Soft delete email messages or clusters, even after they have been delivered
- Quarantine email/attachments: The ability to quarantine emails/attachment is table stakes for mail protection
- Turn off external mail forwarding: Forwarding mail to an external mailbox is a malicious technique that is often used to "spy" on company emails to gather information for a ransomware or phishing campaign. Defender for Office 365 can spot this and turn this functionality off on a mailbox automatically.

There are other capable email hygiene solutions out there, but they don't protect key areas that Defender for Office 365 P2 does–namely, Teams, SharePoint, and OneDrive. This becomes more and more important as your organization scales out use of these services, invites external users into your Teams and SharePoint environments, and allows access to all these environments from devices that you do not directly manage.

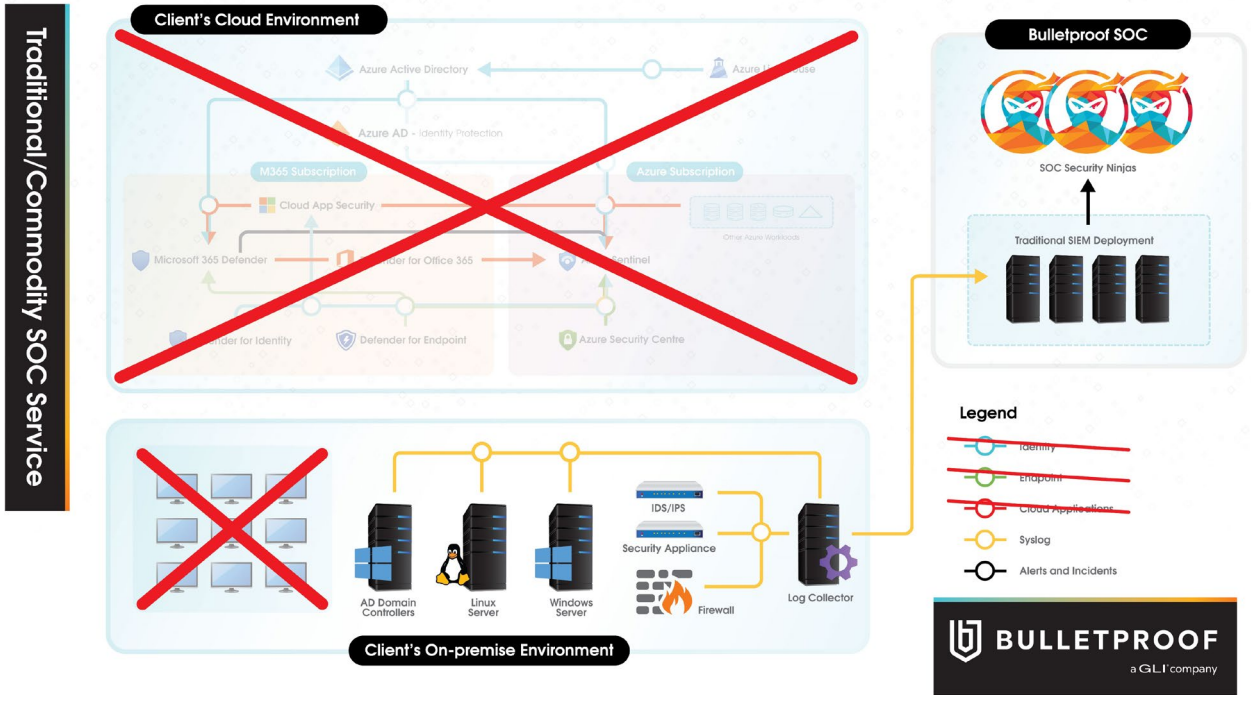
Reduce Risk with Best-of-Platform and Bulletproof 365 Enterprise

Bulletproof 365 Enterprise is architected to provide the most complete security visibility and incident response capabilities possible to meet the requirements of the ever-changing security landscape.

The architecture diagram below illustrates just how integrated this solution is between Microsoft, Bulletproof, and your environment. This integration is the value of our solution; without any one of the components shown below, the integration, and therefore our security monitoring and incident response, suffers, leaving gaps in visibility and control.



Traditional SIEM solutions, which lack integration and deployment of the complete Microsoft E5 Security stack, do not allow the same level of security monitoring and incident response. Legacy SIEM solutions can be appropriate for legacy environments but are not suitable for modern workplaces with modern productivity applications and services.



A modern environment requires a modern security solution, with enhanced investigation and response capabilities. The value of the complete solution with automated response far exceeds what individual "best-of" products can provide for an organization on their own. This reduction in risk is the ROI of the best-of-platform model.

About Bulletproof

Some clouds are silver-lined. Ours is Kevlar. IT experience is one thing; cybersecurity expertise is another.

We are a leading cybersecurity firm with more than two decades of experience in protecting companies around the world. We're also a Microsoft Gold Cloud Partner with 12 Gold competencies:

- Security
- Cloud Platform
- Cloud Productivity
- Data Analytics
- Datacenter
- Messaging
- Application Development
- Windows and Devices
- Application Integration
- Enterprise Mobility Management
- Collaboration and Content
- Small and Midmarket Cloud Solutions

We integrate productivity and security into every solution we develop.

We deliver value, protection, and peace-of-mind that other cloud managed service providers can't.

Gold
Microsoft Partner
Microsoft

2021 Microsoft Global Security Partner of the Year

2019 and **2020 IMPACT Award Winner**: Partner of the Year | Modern Workplace

Member of the **Microsoft Intelligent Security Association**

State-of-the-art 24/7 Security Operations Centre (SOC)

Trusted by users on six continents to protect their data, devices, and people

Automation Across the Entire Platform:
The Modern Security MUST-HAVE

On-Demand Webinar | Chris Simm, Director of Cloud Consulting

Behind every good security product will lie gaps and challenges from configuration to maintenance. Learn the economics of a breach, where to find the most common security blind spots, and how automation can help you keep up with a rapidly changing IT landscape.

WATCH THE WEBINAR

BULLETPROOF
a GLI company

We're here to help solve your complex IT and security problems. **bulletproofsi.com**

TOLL FREE 1.866.328.5538 | INT'L CALL 1.506.452.8558